

TITLE OF THE INVENTION

Web Site Identity Assurance

5 RELATED APPLICATIONS AND CLAIM OF PRIORITY

10 This application claims the benefit of and incorporates
herein by reference the contents of the following co-pending
applications: Application Number 60/279,328 filed March 28,
2001, entitled "Website Identity Assurance"; Application Number
60/289,249 filed on May 7, 2001, entitled "TrustWatch"; and
Application Number 60/295,728 filed on June 4, 2001, entitled
"TrustWatch True Site".

15 BACKGROUND OF THE INVENTION

20 This invention relates to electronic communication systems
and in particular to a method and apparatus for showing end-
users the confirmed identity of a Web site owner, and also in
particular to this method and apparatus being a secure and
reliable reporting mechanism based on existing and prevalent
common standards.

25 The importance of secure communication is increasing as
world-wide networks such as the Internet and the World Wide Web
(WWW) portion of the Internet expand. As global networks expand
through the interconnection of existing networks, users may gain
access to an unprecedented number of services. The services,
each of which may be maintained by a different provider, give
30 users access to academic, business, consumer, and government

information. Service providers are now able to make their services available to an ever-expanding user base that is truly global.

5 The ease with which services and users are able to find each other and the convenience associated with on-line transactions is leading to an increase in the number of remote business and related transactions. However, users and services are not always certain who or what is at the other end of a transaction. Therefore, before they engage in business and other transactions, users and services want and need reassurance that each entity with whom they communicate is who or what it purports to be. For example, users will not be willing to make on-line purchases that require them to reveal their credit card numbers unless they are confident that the service with which they are communicating is in fact the service they wanted to access. Commercial and other private entities who provide on-line services may be more reluctant than individuals to conduct business on-line unless they are confident the communication is with the desired individual or service. From the small and/or new on-line merchant's standpoint, they can reach a global audience through the World Wide Web but they are usually unknown to potential customers and have no brand on which to build an on-line business. For them, displaying confirmed and trusted identity and legitimacy are critical to building their brand and business.

Both users and services need reassurance that neither will compromise the integrity of the other nor that confidential information will be revealed unintentionally to third parties

while communications are occurring. Security in a global network, however, may be difficult to achieve for several reasons. First, the connections between remote users and services are dynamic. With the use of portable devices, users may change their remote physical locations frequently. The individual networks that comprise the global networks have many entry and exit points. Also, packet switching techniques used in global networks result in numerous dynamic paths that are established between participating entities in order to achieve reliable communication between two parties. Finally, communication is often accomplished via inherently insecure facilities such as the public telephone network and many private communication facilities. Secure communication is difficult to achieve in such distributed environments because security breaches may occur at the remote user's site, at the service computer site, or along the communication link. Consequently, reliable two-way authentication of users and the services is essential for achieving security in a distributed environment.

WEBSITE IDENTITY AND SSL PROTOCOL

The problem of establishing the identity of the owner and responsible party for a Web site is partially remedied by protocols such as the Secure Sockets Layer (SSL) protocol.

In the SSL protocol, each communicating program is assigned a key pair consisting of a public cryptographic key and a private cryptographic key. SSL uses the public and private keys for two programs to generate an agreed key that is used to encrypt a conversation between the two programs. This ensures

privacy for the conversation and provides assurance to each party that only the other party could generate the other half of the conversation (this property is called two-party authentication).

5

In these prior art systems, a program that needs to send securely a non-repudiable piece of information (such as a receipt or a signed check) does so by encrypting that piece of information with its private key, which is equivalent to a digital signature. This technique is called signing. The receiver of the signed message can prove that the encrypted information came from the supposed sender (or anyone who knows the sender's private key) by successfully decrypting the message using the sender's public key. The receiver could also forward the message to a third party, who could similarly verify the sender's identity. Thus, non-repudiation is provided for specific situations.

10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
360
370
380
390
400
410
420
430
440
450
460
470
480
490
500
510
520
530
540
550
560
570
580
590
600
610
620
630
640
650
660
670
680
690
700
710
720
730
740
750
760
770
780
790
800
810
820
830
840
850
860
870
880
890
900
910
920
930
940
950
960
970
980
990
1000

20 SSL protocol, therefore, provides a partial identification and authentication solution for Web sites. There are limitations, however, as discussed below.

LIMITATIONS OF SSL PROTOCOL FOR IDENTIFICATION AND AUTHENTICATION

25

Even when a Web site is operating in SSL mode, the identity information stored in the underlying SSL certificate is not easily accessible to an end user for authentication purposes. Further, end users browsing the Web need to be able to know who is behind a site whether in SSL mode or not. Only a small

30

percentage (less than 1%) of Web sites use SSL, and at those sites, only a small percentage (e.g., 1%) of all pages are protected by SSL.

5 In the SSL process the identity of the business responsible for a Web site is established and tied to Web site (actually to the fully qualified domain name) by a trusted certificate authority. This identity, when running under SSL mode, is available in a hidden way by clicking on the lock icon in the browser. However, most users do not know this lock icon is active elements that can be clicked and further do not understand the detailed information provided if they do click on it.

10
15 While SSL does a good job at establishing the basis for identity it has three chief shortcomings: (1) It does not work for pages that are not running under SSL (approximately 99.99% of all Web pages), (2) the identity aspect of SSL is hidden and obscure to the user, and (3) the limited identity information is minimal, incomplete and not considered useful to a consumer.

20
25 Furthermore, while SSL inherently supports identity and encryption, it is primarily focused on encryption. Use of SSL incurs substantial overhead (at least a 35% performance penalty and no possibility of pages being cached), and therefore is only present and usable on pages that require encryption such as those gathering sensitive data. A strategy for taking advantage of the identity aspects of SSL without incurring the overhead of encryption is not possible with its current design which is
30 predicated exclusively on encryption of transmitted data.

NON-SSL WEB SITE IDENTITY SOLUTIONS

While Web sites themselves can assert their identity without the use of SSL (e.g., through simple graphics and text), this identity method also has shortcomings: (1) Each Web site asserts its identity in a different way, leaving the user to figure out how to find the identifying information, and (2) no 3rd party is standing behind the identity assertions, so a Web site can easily deceive an end user by putting whatever identity it desires on the Web site.

USE OF SEALS

Another non-SSL mechanism in common use by Web site owners to establish their identity and legitimacy as a reputable on-line business is to place seals from third parties on some of their Web pages. These seals are meant to portray an endorsement of some kind by the trusted, well-known third party seal provider. Seals are common in the off-line world and are displayed on doors and entrances of storefronts, in yellow page ads, on delivery or work vehicles and so on. On the World Wide Web they take the form of a graphic image and usually an active component such as a link that will identify this site as a legitimate holder in good standing of this seal.

Three serious problems exist with this prevalent mechanism. First, users do not usually click on the seal, which is required to verify association with the seal provider. Since the seal is just a static graphic image pulled from a file resident on the

1
site's Web server, all seals from that provider are identical.
Therefore the only way to differentiate one seal holder from
another and check validity is to click on it. A click usually
transfers the user's browser to the seal provider's site where a
5 page is displayed stating the validity or lack thereof for the
selected seal. Since most users do not click, this check is
rarely performed. Also, users cannot be sure of what the check
really is or what is meant to be displayed, so substituting some
other page intended to represent or simulate validity (but that
10 is actually fraudulent) is a trivial task for someone wanting to
use the seal fraudulently.

11
12
13
14
15
16
17
18
19
20
The second serious issue is seal copying - the hijacking of
the seals and placement on sites that are not legitimately
allowed to display them. Any static image viewed by the browser
is easily saved to a local disk and can be reused in a new Web
page. This copying capability is a fundamental property of
standard Web pages and the browsers that view them. This has
made fraudulent placement of seals on the Web very common. This
fact has made the effectiveness of seals for conveying identity
and legitimacy on the Web weak and ineffective.

21
22
23
24
25
26
27
28
29
30
The third serious issue is Web site spoofing - the
wholesale copying of a Web site to a new location for the
purposes of identity theft and/or fraud. Site spoofing is a
large and growing problem with several very large, public
incidents having occurred and with over 1,000 reported incidents
a year. Current state-of-the-art seals have no ability to detect
site spoofing has occurred. In other words, if a site is spoofed
that has one or more of current generation seals on it, the

visitor to the spoofed site seeing one of these seals will have no indication this is not the legitimate version of that site.

OBJECT OF THE PRESENT INVENTION

5

Accordingly, an object of the present invention is to provide the confirmed identity of a Web site owner and related business information, regardless of whether the end user is browsing under SSL (i.e., in https) or not (i.e., in standard http).

10

It is a further object of the present invention to provide the confirmed identity of the Web site owner and related business information in a standard, recognizable, easy-to-access package passively with no click by the user.

15

It is a further object of the present invention to provide current confirmation that identity and business information is valid and accurate (e.g., not revoked, not expired).

20

It is a further object of the present invention to provide an identity confirmation mechanism that is robust and protects itself from copying or site spoofing threats.

25 SUMMARY OF THE INVENTION

The Web Site Identity Assurance invention described herein provides a confirmed identity and related business information to end users (e.g., browsers). The Identity Assurance is presented to the end user in the form of a visual display on the

30

user's computer desktop or by other means of display or communication. The visual display can be (1) a graphic displayed from a client application tool that an end user would install on his or her machine, (2) a dynamic icon, the code for which is placed on a Web site by the Web site owner, or (3) some other means of display or communication. The client application tool has the ability to watch what sites an end user is browsing and therefore look up the associated confirmed identity information from an independent third party source. The dynamic icon has the ability to cause the browser to look up the associated confirmed identity information from an independent third party source for the URL of the page or pages where the dynamic icon is placed by the Web site owner. All three applications work in both SSL and non-SSL enabled Web sites.

The present invention is a system and method that meets the needs set out above. More particularly, the present invention is a method and system for providing a user with confirmation of the origin of a Web site including the steps of (1) registering a Web site owner's identity and business information with an assuring 3rd party, (2) saving the registration in a database on a registration server, (3) entering in the database the Web site's Internet domain, and cross-referencing the Internet domain to the identity and business information), (4) retrieving the Web site's domain with an Internet browser, (5) calling a program at the assuring 3rd party's registration server via a secure SSL connection and passing it the Internet domain name, (6) determining if the domain has been registered, (7) retrieving from the repository the identity (e.g., official name) and business information cross-referenced to the Internet

domain name and returning the identity and business information to the client tool, (8) displaying the associated identity and business information in the client application tool.

5 In the alternative, the present invention may include the steps of (1) registering a Web site owner's identity and business information with an assuring 3rd party, (2) saving the registration in a database on a registration server, (3) entering in the database the Web site's Internet domain, and
10 cross-referencing the Internet domain to the identity and business information), (4) retrieving the Web site's domain containing an HTML dynamic image tag with an Internet browser, (5) calling a program at the assuring 3rd party's registration server via a secure SSL connection and passing it the Internet domain name, (6) determining if the domain has been registered,
15 (7) retrieving from the repository the identity (e.g., official name) and business information cross-referenced to the Internet domain name and generating an image with the identity and business information contained in the image, (8) displaying the
20 dynamic icon image and associated identity and business information on the browser.

BRIEF DESCRIPTION OF THE DRAWINGS

25 Preferred embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 depicts an exemplary diagram of a network system
30 on which the present invention may be implemented.

Figure 2 depicts an exemplary graphical user interface of a Web Browser.

5 Figure 3 shows the relationship between a standard Web browser and two embodiments of the invention: the dynamic icon embedded in the HTML page displayed by the browser and the confirmed identity active object (client application tool) running on the end user's local computer.

10 Figure 4 shows the 3-way architecture of the client-side application component that reliably displays the confirmed identity of the entity behind the displayed Web.

15 Figure 5 is a more secure option that adds a challenge-response step between the client side application and the Web server that further assures the end user of the identity of the company behind the server.

20 Figure 6 shows the 3-way architecture behind the dynamic icon on the visited Web site that does a lookup of the visited Web site domain on a Secure Assuring 3rd Party Server before the dynamic icon is created and sent from the Secure Assuring 3rd Party Server to the visited Web server.

25 Figure 7 shows the sequence of logical steps behind the confirmed identity algorithm when the client application tool embodiment is activated on a site that is a secured SSL connection (and without reference to information about the site
30 contained on a secure Assuring 3rd Party Server).

Figure 8 depicts an exemplary Web page display incorporating the visual identity assurance display icon of the present invention.

5 Figure 9 depicts an exemplary information window that can be activated by clicking on the Gizmo feature of the present invention.

Figure 10 depicts an embodiment of the Gizmo feature of the present invention further including Credentials information.

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221

Rather, all aspects of the invention can be used with any computer generated content including, but not limited to, rows in a database, an entire database, computer generated queries, documents, and the like.

5

The present invention is preferably implemented using a client server architecture, such as that shown in Figure 1. This architecture includes client 6, certification server 7, and Web server 9 connected via network 10. Network 10 may comprise any type of network or communications medium, including, but not limited to, one or more of the following: the Internet, a local area network ("LAN"), a wide area network ("WAN"), a wireless (e.g., ATM) network, a logical network within a single computer, some other form of programmatic communication such as inter-process communications or dynamic link libraries, or any combination thereof. Client 6 is preferably a personal computer ("PC") or similar data processing device. Client 6 includes network interface 11 for interfacing to network 10, display screen 12 for displaying information to a user, keyboard 14 for inputting text and user commands, mouse 15 for positioning a cursor on display screen 12 and for inputting user commands, disk drive 16 for reading from and writing to floppy disks installed therein, and CD ROM drive 17 for accessing data stored on CD ROM. Close up view 18 shows the internal structure of client 6. Client 6 includes memory 19, which is a computers readable medium, such as a computer hard disk, for storing information. In the preferred embodiment memory 19 stores operating system 20, applications 21, and data 22. Microsoft Windows 2000 is one operating system that may be used with the

invention; however, the invention is not limited to use therewith.

Applications 21 include Web browser 24, among others. An example of a Web browser that may be used with the invention is Netscape™ Navigator Web browser 24 displays a graphical user interface ("GUI") to a user, through which the user may access information via the Internet (e.g., Web sites, individual Web pages, etc.). An example of such a GUI is shown in Figure 2. Client 6 also includes display interface 26, keyboard interface 27, mouse interface 29, disk drive 20 interface 30, CD ROM drive interface 31, computer bus 32, RAM 34, and processor 35. Processor 35 preferably comprises a microprocessor or the like for executing applications, such as those noted above, out of RAM 34. Such applications, including browser 24, may be stored in memory 19 as noted above or, alternatively, on a floppy disk in disk drive 16 or CD ROM in CD ROM drive 17. In this regard, processor 35 accesses applications and data stored on floppy disk via disk drive interface 30 and accesses applications and data stored on CD ROM via CD ROM interface 31. Web server 9 may comprise a computer having features similar to client 6 for providing remote access to the Web site of an organization. Web server 9 is connected to other computers (not shown) in the organization via LAN 36 (or network 10). Web server 9 is also connected to certification server 7 via network 10 or other medium. Web server likewise includes a processor 23 and a memory 28, among other things, as shown in close up view 13.

Stored in this memory is assembly engine 25 and Web page elements 33. Assembly engine 25 is a program that is executed by

processor 23 to assemble Web pages. More specifically, a single Web page may be composed of a plurality of static and dynamic elements, such as images, applets, text, sound, other Web pages, etc. In response to requests received from client 6, assembly engine 25 retrieves those elements (e.g., from memory 28) and combines them in a predetermined manner so as to form the Web page. Representative examples of commercially available assembly engines that may be used in connection with the present invention include ATG Dynamo, Servlets, JSP and ASP.

Certification server 7 likewise preferably comprises a computer having features similar to client 6. As shown in close up view 38, certification server 7 includes, among other things, memory 39 for storing both applications and certification information 48 which includes the manifests described below. Memory 39 may include one or more memory devices, such as a computer hard disk, redundant array of inexpensive disks ("RAID"), optical disk drive, and the like. Processor 40 is also included on certification server 7 so as to execute applications stored in memory 39 and to provide the resulting output to the network.

Among the applications stored in memory 39 is certification engine 41. Certification engine 41 comprises computer executable code that runs on certification server 7 to certify Web pages and other dynamic pages based on their content and/or certification information stored in their elements.

Certification engine 41 also organizes sets of Web pages into plural zones based on their levels of certification, the type of information contained therein, or the like, as described in more detail below. It is noted that certification server 7 and Web server 9 may be one in the same; however, since this is not a requirement, the more general case of separate Web and

certification servers is depicted in Figure 1. For that matter, the invention may also be implemented, in its entirety, on a single computer. That is, the functions of client 6, certification server 7 and Web server 9 (or its equivalent) may be implemented on a single computer.

WEB SITE IDENTITY ASSURANCE

Figures 3 - 10 depict the operation of the Web Site Identity Assurance engine in the context of a particular Web page, although it should be noted that while this embodiment of the invention is described with respect to Web pages, the invention is not limited to use with Web pages and can be used to provide identity assurance of other network data content.

The present invention provides identity assurance of a Web site owner by presenting to the end user in the form of a visual display on the user's computer desktop information regarding the owner. The visual identity display can be either a dynamic icon placed on a Web site by the Web site owner or a graphic displayed from a client application tool that an end user would install on his or her machine. The client application tool has the ability to watch what sites an end user is browsing and therefore look up the associated confirmed identity information.

25

Turning now to Figure 3, there is shown a computer desktop having displayed an exemplary Web page having two alternate representations of the visual identity display. The confirmed site owner name can be, as stated above, a dynamic icon displayed on the owner's Web site, or a display generated by a

client side application, operating outside the Web browser environment. An end user would install on his or her machine the client side application that has the ability to watch what sites an end user is browsing and therefore look up the associated confirmed identity. The operation of the present invention with respect to either alternate identity display will be described in detail with respect to the following figures.

Client Application Tool Example - Assuring 3rd Party Server

Turning now to Figure 4, there is shown a block diagram depicting the process steps for implementing this aspect of the present invention. In this aspect, the operation of the Web site identity assurance method utilizes a client side application and an Assuring 3rd Party Server. The Web Site Identity Assurance is displayed via a client application tool on the end user's desktop. The client application tool is a tool capable of actively monitoring what the end user is browsing and displaying the confirmed identity of the owner of each and every page browsed at that Web site. The operation of the present invention in this embodiment relies on the Assuring 3rd Party Server to provide key information. More specifically the process includes the following steps.

1. At setup time the Web site owner performs an off line registration with an assuring 3rd party. The assuring 3rd party puts an entry in a database cross-referencing the Web Site's Internet domain to the associated identity and business information provided by the Web site owner during registration. The identity and associated business information is

independently confirmed as part of registration. This registration process is a one time event that only occurs at setup time.

2. An end user browses to a Web site that has signed up with the assuring 3rd party. The Web site need not be running under SSL. The client application tool running on the end user's system retrieves the current domain being browsed from the client browser itself.

3. The client application tool calls a program via a secure SSL connection on the Assuring 3rd Party's Server passing it the domain name being browsed.

4. The Assuring 3rd Party Server looks up the domain, determines that it has been registered and returns the associated identity and business information to the client application tool for display.

Client Application Tool Example - Challenge-Response File on Web Site Server

Turning now to Figure 5 there is shown a block diagram depicting the process steps for implementing this aspect of the present invention. In this aspect, the operation of the Web site identity assurance method utilizes an alternative method for displaying to the end user Web Site Identity Assurance using a digitally signed challenge-response file to provide key identity information.

In this alternate version, Web Site Identity Assurance is displayed via a client application tool on the end user's desktop as in the previous exemplary embodiment; however, the identity and business information is stored on the Web site's server rather than the server of the assuring 3rd party. As in the previous example, the client application tool is a tool capable of seeing what the end user is browsing and displaying the confirmed identity and business information of the owner of the Web site. In this embodiment of the present invention, the Assuring 3rd Party Server provides a digitally signed challenge-response file to the Web Site operator to put on the Web Site's server with a known name, for example Identity.txt and in a known location, typically the root directory. More specifically the process includes the following steps.

1. At setup time the Web Site Owner performs an off-line registration with the assuring 3rd party. The assuring 3rd party provides the Web site owner with a challenge-response file containing the identity and business information from registration that has been digitally signed by the assuring 3rd party. This file is placed in a known location on the Web site server. This registration process is a one time event that only occurs at setup time.

2. The user browses to a Web site that has signed up with the assuring 3rd party. The Web site need not be running under SSL. The client application tool running on the end user's system retrieves the current domain being browsed.

3. The client application tool connects to the Web site server looking for the digitally signed file with a known name (for example, Identity.txt) in a known location (typically the root directory).

5

4. The client application tool validates the digital signature of the assuring 3rd party using the embedded 3rd party's public key confirming that the file is not invalid and has not been tampered with. Once confirmed, the client application tool displays the identity and business data obtained from the Assuring 3rd party server.

Dynamic Icon Example

Turning now to Figure 6 there is shown a block diagram depicting the process steps for implementing this aspect of the present invention. In this aspect, the operation of the Web site identity assurance method utilizes a dynamic icon placed on the Web site by the Web site owner without the need for a client application tool as set forth in the exemplary embodiment of Figures 4 and 5. The dynamic icon works similarly to the client application tool; however it is displayed where a Web site owner places it rather than whenever a Web site is browsed to as in the embodiments utilizing a client application tool.

25

1. At setup time the Web Site Owner performs an off-line registration with the assuring 3rd party as previously described.

2. The Web Site Owner places the dynamic icon tag in the desired page(s) on his or her Web Site. The tag is a simple

30

HTML image tag with reference to a remote server not a local static image file as is customary. For example: The image tag might look like <img

src=https://www.thirdparty.com/getImage.jsp>. A very unusual

5 aspect of this is that the image tag points to a program (script) on the Assuring 3rd Party's Server rather than to an actual image. This allows the verification program to be invoked and do the assurance process before creating and returning the dynamic image.

10 3. The user browses to a Web site that has signed up with the assuring 3rd party. The dynamic image icon as described above is embedded in the HTML for the Web site. The browser attempting to render the image will invoke the associated program on the
15 Assuring 3rd Party's Server by transmitting the Internet domain name for the Web site page being viewed by the browser (Referrer Address).

20 4. The Assuring 3rd Party Server program is invoked via a secure https connection.

25 5. The Assuring 3rd Party Server formats the image with the identity and business information associated with the Referrer Address from the data stored in the Assuring 3rd Party Server and adds a date-and-time stamp for copy prevention. The associated program may also return instructions to the browser (e.g., by Java script code) that modifies the behavior of the browser by disabling the right-click or copy function of the end user's mouse so the returned image cannot be copied and pasted at a
30 different Referrer Address (i.e., an anti-fraud and anti-copying

feature). This formatted image containing the associated identity and business information is returned to the Web browser and the Web browser renders the image. This embodiment of the present invention makes use of the standard browser feature -
5 that the browser always provides the domain name of the Web site page being viewed by the browser (Referrer Address) at the time it invokes the program associated with the HTML dynamic image tag embedded on the Web site page - as an additional anti-fraud and identity feature, as the Assuring 3rd Party Server will only
10 render and return an image to the browser containing the registration data for the Referrer Address, and not for any other address. If the HTML dynamic image icon is somehow copied and pasted or otherwise reproduced on a Web page for another domain name, the program will either return no image or a
15 warning image (if the actual domain name is not registered in the Assuring 3rd Party Server) or will return an image containing registration data only for the Web page actually being viewed, not for the Web page from which the HTML dynamic image icon was copied.

20

SSL Only

Turning now to Figure 7 there is shown a block diagram depicting the process steps for implementing this aspect of the
25 present invention. In the circumstance that the end user has entered a Web Site under SSL, and therefore it is a simple matter to implement the features of this invention, to display a confirmed identity for the Web site. More specifically the process includes the following steps.

30

1. The end user browses to a Web site in SSL mode (https).
2. The client application tool recognizes that the browser is in SSL mode, validates the SSL certificate and displays the Organization Name and other embedded information from the certificate.

Visual Identity Assurance Display

Turning now to Figure 8, there is shown an exemplary Web page display incorporating the visual identity assurance display icon. While this feature will be described as being implemented by the client application tool, the features of the visual display described herein are valid to the dynamic icon embodiment as well.

Figure 8 shows an exemplary Web page having a visual identity display, referred to here as a TrustWatch Gizmo. The Gizmo is a visual signal confirming the identity of the owner of the Web page being viewed. In addition, the Gizmo can include in depth information about the owner. Turning to Figure 9 there is shown an exemplary Gizmo information window that can be activated by clicking on the Gizmo displayed in Figure 10. The window can include information regarding the site owner as well as links to further information about the owner. In the exemplary version displayed on Figure 9, there is displayed a window having five buttons listed as; at a glance, company, security, feedback and performance. By selecting any of the buttons, different information will be displayed in the main window. In the exemplary version, there is shown, Company

Information which includes; Name, Address, City State/Region, Postal Code, Telephone, Fax, E-Mail, URL and Links to further information. Additionally, by clicking on one of the other buttons further information will be made available, including
5 details contained in the SSL certificate (if any), information about seals that reside on the Web site, financial data such as credit ratings, credit and payment terms, return policies, ratings by other trading partners and others, the site's privacy and other policy statements, means of providing feedback (e.g.,
10 company contact information and email hyperlinks to appropriate departments), the Web site's relationship to other Web sites (including sites which referred or transferred the end user to the current site being viewed), credit and trustworthiness metrics and scores, and so on.

Turning now to Figure 10, there is shown an alternate embodiment of the TrustWatch Gizmo further including Credentials information. In the depicted embodiment, there is shown three different credentials, Privacy Seals, Security Seals and
20 Reliability Seals, that a site owner could display with regard to a site. Of course it would be obvious to one skilled in the art that various types of credentials can be obtained and displayed and that other type of information could also be displayed under this and other headings. The example shown is
25 not meant to be limiting.

In another embodiment the present invention can be implemented to provide real time confirmation of which Web site a viewer is viewing (i.e., no spoofing or high jacking).
30 Additionally, the user can be provided with confirmation of the

registrant of the domain name and information about the business which owns or is behind the site. The business information could in one embodiment be provided and verified through a variety of independent sources.

5

1. Domain Name Registrant Confirmation

In order to implement this function, enrollment and registration data as is collected as previously described, with the addition of extra fields (as described below). In addition, automatic checking of the domain name registrant against the appropriate registry, such as WHOIS, can be included.

2. Unverified Business Information

The expanded page of True Site can also include unverified business information taken straight from the online enrollment form (no editing). This could also include a text field containing additional information, such as an explanation of the relationship between the "real" business and the site and/or domain name registrant shown in the upper part of True Site.

Information fields would be provided by the business/enrollee as noted as being valid on a particular date. In addition such information would not be independently verified against public records.

The verification of domain name registrant and posting of enrollee business data could then be posted almost immediately on the enrollees site, and begin offering useful information

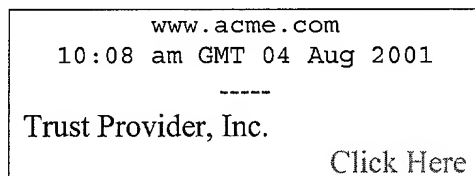
immediately. Operations will not slow the process, and there will be little chance of error.

3. Verified Business Information

5 In an another embodiment of the above process, a standard verification processes for certain data fields in the enrollment form received from the enrollee - chiefly corporate name, official address, state of incorporation, registration number, officers, and renewal date could be undertaken. The True Site
10 display could then be altered to indicate which fields had been independently confirmed. For example, a sentence could be added to the expanded True Site page, as follows "Data fields that have been independently confirmed are marked with an asterisk (*) and the date the data was confirmed." If nothing can be confirmed we no asterisk is shown.

Here is an example of how True Site might look under these rules. First, here it is immediately after enrollment:

20 The True Site icon:



The expanded icon:

✓ Web site identity confirmed

All data shown in this section was independently confirmed by Trust Provider as of 3:54 pm GMT 02 Aug 2001:

Domain name: `www.acme.com`

Domain name registrant:

Acme eCommerce
123 Drive
Chicago, IL 60606 USA

Administrative contact: (John Doe `jdoe@acme.com`)

Registration expires: 25 Jul 2002

Additional business information

The additional business information in this section was provided by `jdoe@acme.com` at 12:26 pm GMT on 01 Aug 2001 and has *not* been independently verified by Trust Provider:

Acme, Inc.
Illinois corporation Registration No. abc 123
Incorporated: 1926
Regis. expires: 26 Mar 2001

123 Drive
Chicago, IL 60606 USA

Telephone: +1.555.555.8732 (General information)

President: Name

Secretary: Name

Registered Agent: Name, Law Firm, Attorneys at Law, X Street,
Chicago, IL 60601

"Acme eCommerce is a wholly owned subsidiary of Acme, Inc. and manages Acme's on-line system."

Your use of this True Site information is governed by these [terms and conditions](#). For more information on True Site and the data displayed, [click here](#).

Later, after we have checked on-line with the Illinois Secretary of State, the expanded icon will appear as follows:

✓Web site identity confirmed

All data shown in this section was independently confirmed by Trust Provider as of 3:54 pm GMT 02 Aug 2001:

Domain name: `www.acme.com`

Domain name registrant:

✓Acme eCommerce, Inc.

✓123 Drive

✓Chicago, IL 60606 USA

✓Administrative contact: (John Doe jdoe@acme.com)

✓Registration expires: 25 Jul 2002

Additional business information

The additional business information in this section was provided by jdoe@acme.com at 12:26 pm GMT on 01 Aug 2001. Data that was independently confirmed by Trust Provider as of 1:37 pm GMT 15 Aug 2001 is marked with a checkmark (✓); none of the other data has been independently confirmed:

✓Acme, Inc.

✓Illinois corporation

✓Registration No. abc 123

Incorporated: 1926

✓Regis. expires: 26 Mar 2001

✓123 Drive

✓Chicago, IL 60606 USA

Telephone: +1.312.555.8732 (General information)

✓President: Name

✓Secretary: Name

✓Registered Agent: Name, Law Firm, Attorneys at Law, 105 State Street, Chicago, IL 60601

"Acme eCommerce is a wholly owned subsidiary of Acme, Inc. and manages Acme's on-line system."

Your use of this True Site information is governed by these [terms and conditions](#). For more information on True Site and the data displayed, [click here](#).

Note that not all information in the display above has a checkmark showing confirmation; nevertheless it is useful. The text field at the end (unconfirmed) is the way a business can explain its relationship to the domain name owner and the domain name itself.

The reason this would work is that the Trust Provider controls the content in a business' True Site on its own computer, so can update these fields and display (including confirmation of fields) whenever it wants to.

The graphics above are just a suggestion - maybe instead confirmed fields get special shading or background. Again, when in doubt, no confirmation would be provided.

Once this kind of True Site is established, it can be expanded over time with more and more tabs and fields with "Trust Provider confirmed" data.

20 Logical Architecture

The techniques described here are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing environment. For example, functions described as being performed by a server can be distributed across different platforms. Moreover, the techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium

readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device and one or more output devices. Program code is applied to data entered using the input device to perform the functions
5 described and to generate output information. The output information is applied to one or more output devices.

Each program is preferably implemented in a high level procedural or object oriented programming language to
10 communicate with a computer system, however, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program is preferably stored on a storage medium or device (e.g., CD-ROM, hard disk or magnetic diskette) that is readable by a general or special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document. The system
15 may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to operate in a specific and predefined manner.

25 Thus, the foregoing descriptions of specific embodiments of the present invention have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, and obviously many modifications and variations are
30 possible in light of the above teaching. The embodiments were

chosen and described in order to best explain the principles of
the invention and its practical application, to thereby enable
others skilled in the art to best utilize the invention and
various embodiments with various modifications as are suited to
5 the particular use contemplated. It is intended that the scope
of the invention be defined by the Claims appended hereto and
their equivalents.